

REMARKS

This Amendment is filed in response to the Office Action dated June 13, 2007, which has a shortened statutory period set to expire September 13, 2007.

Claims 1-41 Are Patentable Over Gray

Applicant respectfully submits that Gray fails to disclose or suggest at least the following, explicitly-identified claim limitations. Specifically, Claim 1 recites, in part (emphasis added),

the request to **initiate a new encryption key derivation being controlled by a MAC sub-layer** and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets.

As taught by Applicant in paragraph [0006] of the Specification, a presentation layer or a session layer is typically used to initiate encrypted communication. The presentation and the session layers are higher OSI (Open System Interconnection) layers than the MAC sub-layer, which forms part of the data link layer. See, e.g. presentation layer 106, session layer 105, and data link layer 102 of Figure 1. As further taught by Applicant in paragraph [0007] of the Specification:

because MAC sub-layer 102A currently does not provide a mechanism to communicate to the higher layer that the key needs to be updated, the higher layer must redundantly store this information, monitor the state of the key (i.e. its location in the key space), and update the key independent of any communication with MAC sub-layer 102A. Moreover, because there is no defined protocol to update the key, the higher layer merely supplants the old key with a new key, thereby causing traffic disruption. Finally, the higher layer does not control communications regarding the data packet granularity (which is provided by MAC sub-layer 102A). Thus, the higher layer is unable to

predict when repetition of nonces occurs (also known as collisions), which can undermine security.

Advantageously, in the recited method for encrypted communications, the request to **initiate a new encryption key derivation is controlled by a MAC sub-layer**. Thus, by using the recited method, the higher layer need not store the information regarding a key that needs updating, monitor the state of the key, or update the key independent of any communication with the MAC sub-layer.

Applicant respectfully submits that Gray fails to teach a MAC sub-layer that initiates derivation of a new key encryption. Indeed, **Gray fails to mention anything regarding a MAC layer, much less its advantages in initiating key encryption**. Because Gray fails to disclose or suggest a request to initiate a new encryption key derivation **being controlled by a MAC sub-layer**, Applicant requests reconsideration and withdrawal of the rejection of Claim 1.

Claims 2-25 depend from Claim 1 and therefore are patentable for at least the reasons presented for Claim 1. Based on those reasons, Applicant requests reconsideration and withdrawal of the rejection of Claims 2-25.

Claim 26 recites in part, "the request to **initiate a new encryption key derivation being controlled by a MAC sub-layer** and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets". Therefore, Claim 26 is patentable for the same reasons presented for Claim 1. Based on those reasons, Applicant requests reconsideration and withdrawal of the rejection of Claim 26.

Claims 27-36 depend from Claim 26 and therefore are patentable for at least the reasons presented for Claim 26. Based on those reasons, Applicant requests reconsideration and withdrawal of the rejection of Claims 27-36.

Claim 37 recites in part, "the request **to initiate a new encryption key derivation being controlled by a MAC sub-layer** and including an exchange threshold indicative of when the new encryption key is to be used to encrypt communication packets". Therefore, Claim 37 is patentable for the same reasons presented for Claim 1. Based on those reasons, Applicant requests reconsideration and withdrawal of the rejection of Claim 37.

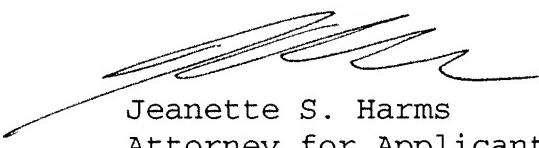
Claims 38-41 depend from Claim 37 and therefore are patentable for at least the reasons presented for Claim 37. Based on those reasons, Applicant requests reconsideration and withdrawal of the rejection of Claims 38-41.

CONCLUSION

Claims 1-41 are pending in the present application.  
Allowance of these claims is respectfully requested.

If there are any questions, please telephone the  
undersigned at 408-451-5907 to expedite prosecution of this  
case.

Respectfully submitted,

  
Jeanette S. Harms  
Attorney for Applicant  
Reg. No. 35,537

Customer No.: 30547